

REMARKS

In response to the Office Action dated November 29, 2005, Applicants respectfully request reconsideration and withdrawal of the rejection of the claims and objections to the disclosure.

The Office Action indicates that the drawings are objected to as containing French text. It appears that the Examiner may be referring to the drawings of the original PCT application, which was published in the French language, rather than the modified drawings that were submitted with the national phase filing of the present application. Those modified drawings comprise seven sheets containing Figures 1-8, in which the original text was translated to English. In the event that the modified drawings cannot be located, duplicate copies of Figures 2, 4 and 7 are being submitted herewith, which contain the translated text.

The drawings were also objected to as allegedly failing to show every feature of the invention in the claims. In particular, the Office Action states that the details of the random data and processing of the random data must be shown. It is respectfully submitted that the processing of the random data is illustrated in the figures. For example, Figure 3 illustrates the manner in which the random value U is combined with the input data D to generate a second random value V. The figure also illustrates that an operation OPN is performed on each of the two random values, and result of these operations are combined by means of an exclusive-OR operation to produce the final result. In a similar manner, Figure 6 illustrates how the random data is processed with respect to a secret key K.

The Office Action also refers to the "details" of the random data. It is not understood what is being requested by this term. The only detail of the random data

that is recited in the claims is the fact that the random data has the same size as an input data item. This detail is explicitly identified in Figure 6, for example, where both the random value Y and the key K are identified as having a length of 64 bits.

Accordingly, it is respectfully submitted that the drawings illustrate the features of the invention that are specified in the claims. Withdrawal of the objection on this basis is respectfully requested.

Claims 6-8 and 15-18 were objected to as containing informalities in connection with certain terminology. In view of the cancellation of these claims, the basis for the objection has been removed.

Claims 1-8, 10 and 13-23 were rejected under 35 U.S.C. § 102, on the grounds that they were considered to be anticipated by the Kocher et al patent (US 6,278,783). To clarify the distinctions between the disclosure of the Kocher patent and the subject matter of the present application, the rejected claims have been canceled and new claims 24-37 are presented herein.

Like the present invention, the Kocher patent is concerned with thwarting attacks on the security of cryptographic operations. However, the particular approach that is described in the Kocher patent differs from that of the present application. More particularly, as illustrated in the flowchart of Figure 2, the Kocher patent discloses that random values are employed in connection with the S-table look-up operation of the DES algorithm. In contrast, in accordance with one embodiment of the invention illustrated in Figure 4, a random value is employed in connection with at least one of the permutation operations that is carried out before or after the table look-up operation (SBOX). The particular manner in which the random value is processed during those permutation operations is depicted in Figure

3. Specifically, the random value U is combined with the data D to be permuted to form another random value V. Then each of the random values U and V undergoes the permutation operation. The results of these two operations are then combined by means of an exclusive-OR operation.


New claim 24 recites that, for a plurality of successive rounds of the DES algorithm, at least one of the two permutation operations comprises the steps of selecting a first random value, and performing an exclusive-OR operation between that first random value and the data being permuted, to generate a second random value. The permutation operation is then executed on each of these two random values, and an exclusive-OR operation is performed on the results of the permutation operations, to produce a final permuted result. Further features of this sequence of operations are set forth in dependent claims 25-27. Claims 28-30 recite a further feature of the invention, in which a random value is utilized in connection with the secret key K, to generate a pair of intermediate keys that are used to manipulate the data in a round of the algorithm, as depicted in Figures 6 and 7. New claims 31-37 recite an electronic component having a microprocessor that executes the operations associated with this countermeasure.

It is respectfully submitted that the subject matter of claims 24-37 is not disclosed by the Kocher patent. Reconsideration and withdrawal of the rejection based upon this patent is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: March 29, 2006

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620